UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/872,077	06/01/2001	Lisa Amini	STL920000116US1	3841

24852 7590 06/20/2006

INTERNATIONAL BUSINESS MACHINES CORP
IP LAW
555 BAILEY AVENUE , J46/G4
SAN JOSE, CA 95141

EXAMINER	
NALVEN, ANDREW L	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/872,077	AMINI ET AL.	
	Examiner	Art Unit	
	Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,15-20,23,24 and 37-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12, 15-20, 23-24, 37-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12, 15-20, 23-34, and 37-42 are pending.

Response to Arguments

2. Applicant's arguments filed 12 April 2006 have been fully considered but they are not persuasive.

3. Applicant has argued on page 12 that the Shimomura reference acts contrary to the claimed recitations provided in Claim 1. Applicant asserts that the claims provide that "if a previous data element was lost or altered, the claimed invention decrypts a subsequent data element and does not recover the previous data element." Applicant asserts that this functionality conflicts with Shimomura's error correction scheme where data that has underwent a transmission failure is corrected. Examiner respectfully disagrees. Claim 1 only provides that no retransmission is attempted after a transmission failure and in no way states that recovery does not occur. Shimomura teaches that no retransmission is necessary because the disclosed error correction procedures obviate the need for retransmission.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

> art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1-12, 15-20, 23-34, and 37-42 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The cited claims provide limitations stating "in response to a transmission failure of a previous data element, said data element also being decrypted with said encryption state, without retransmission of the previous data element." The specification fails to provide adequate support for the decryption of a data element where the previous data element transmission failed.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-5, 7-10, 12, 15-18, 20, 23-27, 29-32, 34, 37-40, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mitty et al US Patent No. 6,145,079 in view of Shimomura et al US Patent No. 6,473,858 and Liechti et al US Patent No. 5,715,164.

7. With regards to claims 1, 7, 15, 23, 29 and 37, Mitty teaches a data element being statically encrypted with a static key (Mitty, column 8 lines 48-51, M2 encrypted to form M3), a data element being dynamically encrypted with a dynamic key (Mitty, column 12 lines 14-23, M9 encrypted to form M10), and a data element being decrypted with a dynamic key and a static key (Mitty, column 12 line 61 – column 13 line 17, decrypts M10 and M3). Mitty fails to teach that in response to a transmission failure of said data element, decryption of said data element being recovered without retransmission of data and the use of encryption states. However, Liechti teaches an encryption state being associated with said data element being statically encrypted with said static key (Liechti, column 8 lines 17-29, key and value which is function of a previous block). Further, Shimomura teaches that in response to a transmission failure of said data element, decryption of said data element being recovered without retransmission of data (Shimomura, column 14 lines 5-15) thus allowing decryption of a subsequent block to take place even if there was a transmission failure. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Shimomura's correction method and Liechti's encryption state method with Mitty's secure transaction system because it offers the advantage of ensuring that received data is not lost or altered (Shimomura, column 14 lines 5-15) and helps hide repeated patterns in encrypted data which helps defeat attempts at cryptanalysis (Liechti, column 1 lines 49-59).

8. With regards to claims 2, 8, 16, 24, 30, 38, Mitty as modified teaches encryption with said static key being strong encryption (Mitty, column 8 lines 48-51).

9. With regards to claims 3, 9, 17, 25, 31, 39, Mitty as modified teaches encryption with said dynamic key being weak encryption (Mitty, column 12 lines 14-23).

10. With regards to claims 4, 10, 18, 26, 32, 40, Mitty as modified teaches a data element being encrypted with a static key on a first computer system (Mitty, column 8 lines 48-51, M2 encrypted to form M3, column 10 lines 9-16 intermediary receives package from sender), the data element being encrypted with the dynamic key on a second computer system (Mitty, column 12 lines 14-23, M9 encrypted to form M10 by intermediary computer system), and the data element being decrypted with the static key and dynamic key on a third computer system thereby encryption and decryption are distributed between the first, second, and third computer systems (Mitty, column 12 line 61 – column 13 line 17, recipient/3rd computer system decrypts M10 and M3).

11. With regards to claims 5 and 27, Mitty as modified fails to teach the second computer being untrusted. Examiner contends that untrusted computers are well known in the art and it would have been obvious to a person of ordinary skill in the art to allow Mitty's system to work with untrusted computers because it offers the advantage of allowing interoperability with a far wider range of networks and systems.

12. With regards to claims 12, 20, 34 and 42, Mitty as modified teaches the determination of whether a transmission failed (Mitty, column 6 lines 30-56, confirmation messages) and the repairing of the data element without retransmission (Shimomura, column 14 lines 5-15).

13. Claims 6, 11, 19, 28, 33, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mitty et al US Patent No. 6,145,079, Shimomura et al US Patent No. 6,473,858, and Liechti et al US Patent No. 5,715,164, as applied to claims 1, 7, 15, 23, 29, and 37, in further view of Bailey III US Patent No. 5,659,614.

14. With regards to claims 6, 11, 19, 28, 33, and 41, Mitty as modified teaches a data element being encrypted with a static key and a dynamic key on a first computer system (Mitty, column 8 lines 48-51, M2 encrypted to form M3, column 9 lines 25-47 encrypted M5 to form M6), but fails to teach the data element being decrypted by the same dynamic key on a second computer system. Bailey teaches the data element being decrypted with the static key and the dynamic key on a second computer system (Bailey, column 6 lines 9-21, column 18 lines 53-55). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Bailey's method with Mitty's secure transaction system because it offers the advantage of helping ensure an attacker cannot decrypt data by acquiring a single key during a transmission from a source to destination (Bailey, column 6 lines 8-21).

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on 571 272 6962. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

JACQUES H. LOUIS-JACQUES
PRIMARY EXAMINER